円分体$\mathbb{Q}(\zeta_p)$のベクトル空間としての性質について

児玉　英一郎

1. はじめに

自然数mに対して，$x^m-1=0$の根を1のm乗根という．1のm乗根全体は，乗法に関して位数mの巡回群をなす，その生成元を1の原始m乗根とよび，記号ζ_mで表す．1の原始m乗根は，$\varphi(m)$個(φはオイラー関数)あり，$e^{\frac{2\pi i}{m}k}=e(2\pi ik/m),(k,m)=1$である．

例えば，$m=4$の場合，$x^4-1=0$の根は，$1,-1,i,-i$であり，$\zeta_4=i$と書くことができ，$\langle i\rangle=\{i,i^2=-1,i^3=-i,i^4=1\}$となる．

また，$m=7$の場合，$x^7-1=0$の根は，$\zeta_7=e^{\frac{2\pi i}{7}}=e(2\pi i/7)$とすると，$\zeta_7^n=e(2\pi in/7),n=0,1,2,3,4,5,6$である．すなわち，$\zeta_7=e(2\pi i/7)=\cos\frac{2\pi}{7}+i\sin\frac{2\pi}{7}$とすると，$\langle\zeta_7\rangle=\{1,\zeta_7,\zeta_7^2,\zeta_7^3,\zeta_7^4,\zeta_7^5,\zeta_7^6\}$となる．

1の原始m乗根全体を根にもつ$\varphi(m)$次の多項式

$$\Phi_m(x)=\prod_k(x-\zeta_m^k),\qquad (\overline{k}\in(\mathbb{Z}/m\mathbb{Z})^\times)$$

を円分多項式と呼ぶ．

$\mu(n)$をメービウス関数

$$\mu(n)=\begin{cases}1 & n=1\\ (-1)^r & n=p_1p_2\cdots p_r\\ 0 & p^2|n\end{cases}$$

とするとき，円分多項式は次の性質を持つ．

$$\Phi_m(x)=\prod_{d|m}(x^d-1)^{\mu(m/d)}$$

例えば，$m=12$の場合，$d=1,2,3,4,6,12$となり，$\mu(1)=1,\mu(2)=-1,\mu(3)=-1,\mu(4)=0,\mu(6)=1,\mu(12)=0$であるから，

$\Phi_{12}(x)=(x^2-1)(x^4-1)^{-1}(x^6-1)^{-1}(x^{12}-1)=x^4-x^2+1$となる．

1のm乗根を集めた集合をP_mとすると，$P_m=\{e(2\pi ik/m)|k=0,1,\cdots,m-1\}$と書くことができ，$|P_m|=m$である．

また，1の原始m乗根を集めた集合をQ_mとすると，$Q_m=\{e(2\pi ik/m)|k=0,1,\cdots,m-1,\ (k,m)=1\}$と書くことができ，$|Q_m|=\varphi(m)$である．一方で，$d|m$なる$d$に対して，1の原始$d$乗根は$m$乗すると1となるから1の$m$乗根の一つである．従って，$P_m\supseteq\bigcup_{d|m}Q_d$となる．

ここで，$|Q_d|=\varphi(d),\sum_{d|m}\varphi(d)=m$であること，$d,d'|m$なる$d,d'$に対して，$d\neq d'\Rightarrow Q_d\cap Q_{d'}=\emptyset$であることより，$\left|\bigcup_{d|m}Q_d\right|=\sum_{d|m}|Q_d|=m$となり，$P_m=\bigcup_{d|m}Q_d$であることが分かる．$P_m$の要素は，$x^m-1=0$の根であり，$Q_d$の要素は，$\Phi_d(x)=0$の根であるから，$x^m-1=\prod_{d|m}\Phi_d(x)$となる．

この性質を使って円分多項式を求めると，表1のようになる．

表1　円分多項式

m	$\Phi_m(x)$
1	$\Phi_1(x)=x-1$
2	$\Phi_2(x)=x+1$
3	$\Phi_3(x)=x^2+x+1$
4	$\Phi_4(x)=x^2+1$
5	$\Phi_5(x)=x^4+x^3+x^2+x+1$
6	$\Phi_6(x)=x^2-x+1$
7	$\Phi_7(x)=x^6+x^5+x^4+x^3+x^2+x+1$
8	$\Phi_8(x)=x^4+1$
9	$\Phi_9(x)=x^6+x^3+1$
10	$\Phi_{10}(x)=x^4-x^3+x^2-x+1$
11	$\Phi_{11}(x)=x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$
12	$\Phi_7(x)=x^4-x^2+1$
13	$\Phi_{13}(x)=x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$
14	$\Phi_{14}(x)=x^6-x^5+x^4-x^3+x^2-x+1$
15	$\Phi_{15}(x)=x^8-x^7+x^5-x^4+x^3-x+1$
16	$\Phi_{15}(x)=x^8+1$

2. 円分体

2.1. 円分体の定義と性質

有理数体$\mathbb{Q}$に1の原始m乗根ζ_mを添加してできる体$\mathbb{Q}(\zeta_m)$を円のm分体(円分体)と呼ぶ.

円分体$\mathbb{Q}(\zeta_m)$は$\mathbb{Q}$上の$\varphi(m)$次のベクトル空間であり，$\mathbb{Q}(\zeta_m)/\mathbb{Q}$の拡大次数$[\mathbb{Q}(\zeta_m):\mathbb{Q}]$は$\varphi(m)$となる.

また，$\mathbb{Q}(\zeta_m)/\mathbb{Q}$は，Galois 拡大で，その Galois 群$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$は，以下の自己同型写像からなる.

$$\sigma_j:\zeta_m \mapsto \zeta_m^j, \qquad (j,m)=1$$

ここで，$jk \equiv l \pmod m$とすると，

$$\sigma_j\sigma_k = \sigma_l$$

となるから,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong \left(\mathbb{Z}/m\mathbb{Z}\right)^\times$$

である.

$\left(\mathbb{Z}/m\mathbb{Z}\right)^\times$は，Abel 群であり，$m$が素数$p$の場合には巡回群となるから，円分体$\mathbb{Q}(\zeta_m)$は Abel 拡大であり，特に，素数$p$に対しては，巡回拡大となる.

一方，Kronecker によって，$\mathbb{Q}$上の Abel 拡大は，必ず，ある円分体の部分体になることが知られている．例えば，2 次体$\mathbb{Q}(\sqrt{\pm m})$は，円分体$\mathbb{Q}(\zeta_{4m}) = \mathbb{Q}(\sqrt{-1},\zeta_m)$に含まれる．場合を分けて詳しく見ると，次のことが知られている.

・$\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\zeta_8), \mathbb{Q}(\sqrt{-2}) \subset \mathbb{Q}(\zeta_8)$

・素数pに対して，$p \equiv 1 \pmod 4$の場合,

$\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_p), \mathbb{Q}(\sqrt{-p}) \subset \mathbb{Q}(\zeta_{4p})$

・素数pに対して，$p \equiv 3 \pmod 4$の場合,

$\mathbb{Q}(\sqrt{-p}) \subset \mathbb{Q}(\zeta_p), \mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_{4p})$

2.2. 円分体の例

$m = 3,4$の場合で見てみると，$m = 3$のとき，$\Phi_3(x) = x^2 + x + 1$であり，$\zeta_3 = e(2\pi i/3)$とすると，$\zeta_3 = e(2\pi i/3) = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = \frac{-1+\sqrt{3}i}{2}$であるため，$\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$となり，虚 2 次体となる.

$m = 4$のとき，$\Phi_4(x) = x^2 + 1$であり，$\zeta_4 = \sqrt{-1}$とすると，$\mathbb{Q}(\zeta_4) = \mathbb{Q}(\sqrt{-1})$となり，ガウス数体となる.

$m = 5$の場合には，$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$であり，$\zeta_5 = e(2\pi i/5) = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$とすると，$\mathbb{Q}(\zeta_5)$は，$\mathbb{Q}$上の 4 次体となる.

剰余群$\left(\mathbb{Z}/5\mathbb{Z}\right)^\times = \{\bar{1},\bar{2},\bar{3},\bar{4}\}$は，位数 2 の部分群$\{\bar{1},\bar{4}\}$を持つから，Galois 理論によって，ガロア拡大$\mathbb{Q}(\zeta_5)/\mathbb{Q}$は，部分体として$\mathbb{Q}$上の 2 次体を含む．この 2 次体は，$\mathbb{Q}(\sqrt{5})$である.

一方で，$\mathbb{Q}(\sqrt{-5})$は，$\mathbb{Q}(\zeta_{20})$の部分体となる．剰余群$\left(\mathbb{Z}/20\mathbb{Z}\right)^\times$について考えると，

$\varphi(20) = \varphi(4)\cdot\varphi(5) = (2^2-2)\cdot(5-1) = 8$

であり，$\left(\mathbb{Z}/20\mathbb{Z}\right)^\times = \{\bar{1},\bar{3},\bar{7},\bar{9},\overline{11},\overline{13},\overline{17},\overline{19}\}$となる.

$\left(\mathbb{Z}/20\mathbb{Z}\right)^\times$は，自明でない部分群として，位数 4 と位数 2 の部分群を持つ．この部分群を以下に示す.

・位数 4 の部分群：

$$\langle\bar{3}\rangle = \{\bar{1},\bar{3},\bar{7},\bar{9}\}, V = \{\bar{1},\bar{9},\overline{11},\overline{19}\},$$
$$\langle\overline{13}\rangle = \{\bar{1},\bar{9},\overline{13},\overline{17}\}$$

・位数 2 の部分群：

$$\langle\bar{9}\rangle = \{\bar{1},\bar{9}\}, \langle\overline{11}\rangle = \{\bar{1},\overline{11}\}, \langle\overline{19}\rangle = \{\bar{1},\overline{19}\}$$

ここで，Vは，クラインの 4 元群である.

このことから，$\mathbb{Q}(\zeta_{20})$は，3 つの$\mathbb{Q}$上の 2 次体と，3 つの$\mathbb{Q}$上の 4 次体を含むことが分かる．それらを以下に示す.

・$\mathbb{Q}(\zeta_{20})$に部分体として含まれる 2 次体：

$$\mathbb{Q}(\sqrt{-5}), \mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{-1})$$

・$\mathbb{Q}(\zeta_{20})$に部分体として含まれる 4 次体：

$$\mathbb{Q}(\sqrt{-1},\sqrt{5}), \mathbb{Q}(\zeta_5), \mathbb{Q}\left(\sqrt{\frac{5+\sqrt{5}}{2}}\right)$$

$m = 7$の場合には，$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$であり，$\zeta_7 = e(2\pi i/7) = \cos\frac{2\pi}{7} + i\sin\frac{2\pi}{7}$とすると，$\mathbb{Q}(\zeta_7)$は，$\mathbb{Q}$上の 6 次体となる.

剰余群$\left(\mathbb{Z}/7\mathbb{Z}\right)^\times = \{\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6}\}$は，位数 2 の部分群$\{\bar{1},\bar{6}\}$と，位数 3 の部分群$\{\bar{1},\bar{2},\bar{4}\}$を持つから，Galois 理論によって，ガロア拡大$\mathbb{Q}(\zeta_7)/\mathbb{Q}$は，部分体として，$\mathbb{Q}$上の 3 次体と 2 次体を含む．この 2 次体は$\mathbb{Q}(\sqrt{-7})$であり，3 次体は$\mathbb{Q}(\zeta_7+\zeta_7^{-1}) = \mathbb{Q}\left(2\cos\frac{2\pi}{7}\right)$となる.

3. Gauss sum

3.1. Legendre の平方剰余記号

$x^2 \equiv a \pmod m$, $(a,m)=1$がxについて整数解をもつとき，aをmを法とする平方剰余といい，そうでないとき，aをmを法とする非平方剰余という．素数pと整数$a,(a,p)=1$に対して，aがpを法とする平方剰余であるとき，

$$\left(\frac{a}{p}\right)=1$$

aがpを法とする平方剰余であるとき，

$$\left(\frac{a}{p}\right)=-1$$

と表し，これを，Legendre の平方剰余記号と呼ぶ．

以下，Legendre の平方剰余記号の性質を示す．

・$a \equiv b \pmod p$, $(a,p)=1$, $(b,p)=1$ならば，

$$\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$$

・$(a,p)=1$のとき，$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$,

・$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

・$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

・$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$

・$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$

この性質によって$\left(\frac{5}{7}\right)$や$\left(\frac{13}{19}\right)$を求めてみる．

$\left(\frac{5}{7}\right)\left(\frac{7}{5}\right)=(-1)^{\frac{5-1}{2}\cdot\frac{7-1}{2}}=1$，従って，$\left(\frac{5}{7}\right)=\left(\frac{7}{5}\right)=\left(\frac{2}{5}\right)=(-1)^{\frac{25-1}{8}}=-1$となる．

同じく，$\left(\frac{13}{19}\right)\left(\frac{19}{13}\right)=(-1)^{\frac{13-1}{2}\cdot\frac{19-1}{2}}=1$，従って，

$\left(\frac{13}{19}\right)=\left(\frac{19}{13}\right)=\left(\frac{6}{13}\right)=\left(\frac{2}{13}\right)\left(\frac{3}{13}\right)=(-1)^{\frac{169-1}{8}}\left(\frac{3}{13}\right)=-\left(\frac{3}{13}\right)$となる．$\left(\frac{3}{13}\right)\left(\frac{13}{3}\right)=(-1)^{\frac{3-1}{2}\cdot\frac{13-1}{2}}=1$より，$\left(\frac{3}{13}\right)=\left(\frac{13}{3}\right)=\left(\frac{1}{3}\right)=1$．従って，$\left(\frac{13}{19}\right)=-1$となる．

3.2. Gauss sum の定義と例

Legendre の平方剰余記号を用い記述された

$$\mathrm{G}(\zeta_p)=\zeta_p+\left(\frac{2}{p}\right)\zeta_p^2+\cdots+\left(\frac{p-1}{p}\right)\zeta_p^{p-1}$$

を Gauss sum と呼ぶ．$p=3,5,7,11,13$の場合の Gauss sum を表 2 に示す．

表 2　Gauss sum

p	Gauss sum
3	$\mathrm{G}(\zeta_3)=\zeta_3-\zeta_3^2=\sqrt{-3}$
5	$\mathrm{G}(\zeta_5)=\zeta_5-\zeta_5^2-\zeta_5^3+\zeta_5^4=\sqrt{5}$
7	$\mathrm{G}(\zeta_7)=\zeta_7+\zeta_7^2-\zeta_7^3+\zeta_7^4-\zeta_7^5-\zeta_7^6$ $=\sqrt{-7}$
11	$\mathrm{G}(\zeta_{11})=\zeta_{11}-\zeta_{11}^2+\zeta_{11}^3+\zeta_{11}^4+\zeta_{11}^5-\zeta_{11}^6$ $-\zeta_{11}^7-\zeta_{11}^8+\zeta_{11}^9-\zeta_{11}^{10}=\sqrt{-11}$
13	$\mathrm{G}(\zeta_{13})=\zeta_{13}-\zeta_{13}^2+\zeta_{13}^3+\zeta_{13}^4-\zeta_{13}^5-\zeta_{13}^6$ $-\zeta_{13}^7-\zeta_{13}^8+\zeta_{13}^9+\zeta_{13}^{10}-\zeta_{13}^{11}+\zeta_{13}^{12}=\sqrt{13}$

この Gauss sum に関しては，次の性質が知られている．

・$\mathrm{G}(\zeta_p)=\sum_{x=0}^{p-1}\zeta_p^{x^2}$

・$\mathrm{G}(\zeta_p)^2=\left(\frac{-1}{p}\right)p$

・$\mathrm{G}(\zeta_p)=(\zeta_p-\zeta_p^{-1})(\zeta_p^3-\zeta_p^{-3})\cdots(\zeta_p^{p-2}-\zeta_p^{-(p-2)})$

・$\mathrm{G}(\zeta_p)=\begin{cases}\sqrt{p} & p\equiv 1 \pmod 4\\ \sqrt{-p} & p\equiv 3 \pmod 4\end{cases}$

この第 1 の性質からも，以下のことが分かる．

$\mathrm{G}(\zeta_7)=\zeta_7^0+\zeta_7^1+\zeta_7^4+\zeta_7^9+\zeta_7^{16}+\zeta_7^{25}+\zeta_7^{36}$

$=1+\zeta_7+\zeta_7^4+\zeta_7^2+\zeta_7^2+\zeta_7^4+\zeta_7$

$=1+2\zeta_7+2\zeta_7^2+2\zeta_7^4$

$=(-\zeta_7-\zeta_7^2-\zeta_7^3-\zeta_7^4-\zeta_7^5-\zeta_7^6)+2\zeta_7+2\zeta_7^2+2\zeta_7^4$

$=\zeta_7+\zeta_7^2-\zeta_7^3+\zeta_7^4-\zeta_7^5-\zeta_7^6$

また，第 3 の性質によって，

$\mathrm{G}(\zeta_3)=\zeta_3-\zeta_3^{-1}$,

$\mathrm{G}(\zeta_5)=(\zeta_5-\zeta_5^{-1})(\zeta_5^3-\zeta_5^{-3})$,

$\mathrm{G}(\zeta_7)=(\zeta_7-\zeta_7^{-1})(\zeta_7^3-\zeta_7^{-3})(\zeta_7^5-\zeta_7^{-5})$

と記述できることも分かる．

そして，第 4 の性質から，

$\mathrm{G}(\zeta_3)=\sqrt{-3}$, $\mathrm{G}(\zeta_5)=\sqrt{5}$, $\mathrm{G}(\zeta_7)=\sqrt{-7}$,

$\mathrm{G}(\zeta_{11})=\sqrt{-11}$, $\mathrm{G}(\zeta_{13})=\sqrt{13}$

であることが分かる．

4. ベクトル空間としての$\mathbb{Q}(\zeta_p)$

円分体$\mathbb{Q}(\zeta_p)$は，$\mathbb{Q}$上の$\varphi(p)$次元のベクトル空間であり，部分空間として，$p \equiv 1 \pmod 4$の場合には，$\mathbb{Q}(\sqrt{p})$を含み，$p \equiv 3 \pmod 4$の場合には，$\mathbb{Q}(\sqrt{-p})$を含んでいる．

例えば，$p = 5$の場合，$\mathbb{Q}(\zeta_5)$は，$\mathbb{Q}$上の 4 次元のベクトル空間であり，その 1 組の基底は，$1, \zeta_5, \zeta_5^2, \zeta_5^3$である．そして，部分空間として，$\mathbb{Q}(\sqrt{5})$を含んでいる．$\mathbb{Q}$上の 2 次元ベクトル空間$\mathbb{Q}(\sqrt{5})$の 1 組の基底は，$1, \sqrt{5}$である．$\mathbb{Q}(\zeta_5)$は，$\mathbb{Q}(\sqrt{5})$上から見ると 2 次元のベクトル空間となっており，その一組の基底は，例えば，$1, \zeta_5$と取ることができる．実際，任意の$a + b\sqrt{5}, c + d\sqrt{5} \in \mathbb{Q}(\sqrt{5})$に対して，$\mathbb{Q}(\sqrt{5})$上の線形結合$(a + b\sqrt{5}) \cdot 1 + (c + d\sqrt{5}) \cdot \zeta_5$を考え，

$$(a + b\sqrt{5}) \cdot 1 + (c + d\sqrt{5}) \cdot \zeta_5 = 0$$

とすると，Gauss sum によって，

$$\sqrt{5} = \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4$$

であり，

$$1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = 0$$

より，

$$\zeta_5^4 = -1 - \zeta_5 - \zeta_5^2 - \zeta_5^3$$

であるから，

$$\sqrt{5} = -1 - 2\zeta_5^2 - 2\zeta_5^3$$

となる．従って，

$$\left(a + b(-1 - 2\zeta_5^2 - 2\zeta_5^3)\right) \cdot 1 + \left(c + d(-1 - 2\zeta_5^2 - 2\zeta_5^3)\right) \cdot \zeta_5 = 0$$

となる．整理すると，

$$a - b - 2b\zeta_5^2 - 2b\zeta_5^3 + (c - d - 2d\zeta_5^2 - 2d\zeta_5^3) \cdot \zeta_5 = 0,$$

$$a - b - 2b\zeta_5^2 - 2b\zeta_5^3 + (c - d)\zeta_5 - 2d\zeta_5^3 - 2d\zeta_5^4 = 0,$$

$$(a - b) + (c - d)\zeta_5 - 2b\zeta_5^2 + (-2b - 2d)\zeta_5^3 - 2d(-1 - \zeta_5 - \zeta_5^2 - \zeta_5^3) = 0,$$

$$(a - b + 2d) + (c + d)\zeta_5 + (-2b + 2d)\zeta_5^2 - 2b\zeta_5^3 = 0$$

となる．$1, \zeta_5, \zeta_5^2, \zeta_5^3$は，$\mathbb{Q}$上線形独立であるため，$a = b = c = d = 0$となり，$a + b\sqrt{5} = c + d\sqrt{5} = 0$となる．従って，$1, \zeta_5$は，$\mathbb{Q}(\sqrt{5})$上線形独立であり，ベクトル空間$\mathbb{Q}(\zeta_5)/\mathbb{Q}(\sqrt{5})$の一組の基底となることが分かる．

実際，$\sqrt{5} = -1 - 2\zeta_5^2 - 2\zeta_5^3$より，$\sqrt{5}\zeta_5 = -\zeta_5 - 2\zeta_5^3 - 2\zeta_5^4$となり，$\sqrt{5}\zeta_5 = -\zeta_5 - 2\zeta_5^3 - 2(-1 - \zeta_5 - \zeta_5^2 - \zeta_5^3)$となる．従って，$\sqrt{5}\zeta_5 = -\zeta_5 - 2\zeta_5^3 + 2 + 2\zeta_5 + 2\zeta_5^2 + 2\zeta_5^3$，$\sqrt{5}\zeta_5 = 2 + \zeta_5 + 2\zeta_5^2$となる．

このことから，

$$\zeta_5^2 = -1 + \frac{(-1 + \sqrt{5})}{2}\zeta_5$$

となる．同様に，

$$\zeta_5^3 = \zeta_5^2 \cdot \zeta_5 = \left(-1 + \frac{(-1 + \sqrt{5})}{2}\zeta_5\right) \cdot \zeta_5$$

$$= -\zeta_5 + \frac{(-1 + \sqrt{5})}{2}\zeta_5^2$$

$$= -\zeta_5 + \frac{(-1 + \sqrt{5})}{2}\left(-1 + \frac{(-1 + \sqrt{5})}{2}\zeta_5\right)$$

$$= -\zeta_5 - \frac{(-1 + \sqrt{5})}{2} + \left(\frac{-1 + \sqrt{5}}{2}\right)^2 \zeta_5$$

$$= -\zeta_5 - \frac{(-1 + \sqrt{5})}{2} + \frac{6 - 2\sqrt{5}}{4}\zeta_5$$

$$= \frac{1 - \sqrt{5}}{2} + \frac{1 - \sqrt{5}}{2}\zeta_5$$

となり，ζ_5^3も$\mathbb{Q}(\sqrt{5})$上$1, \zeta_5$で表現できる．このことから，$\mathbb{Q}(\zeta_5)$の任意の要素$(a + b\zeta_5 + c\zeta_5^2 + d\zeta_5^3, a, b, c, d \in \mathbb{Q})$が$\mathbb{Q}(\sqrt{5})$上では，$1, \zeta_5$の線形結合として表現できることが分かる．

$p = 7$の場合，$\mathbb{Q}(\zeta_7)$は，$\mathbb{Q}$上の 6 次元のベクトル空間であり，その 1 組の基底は，$1, \zeta_7, \zeta_7^2, \zeta_7^3, \zeta_7^4, \zeta_7^5$である．そして，部分空間として，$\mathbb{Q}(\sqrt{-7})$を含んでいる．$\mathbb{Q}$上の 2 次元ベクトル空間$\mathbb{Q}(\sqrt{-7})$の 1 組の基底は，$1, \sqrt{-7}$である．$\mathbb{Q}(\zeta_7)$は，$\mathbb{Q}(\sqrt{-7})$上から見ると 3 次元のベクトル空間となっている．また，部分空間として，$\mathbb{Q}(\zeta_7 + \zeta_7^{-1}) = \mathbb{Q}\left(2\cos\frac{2\pi}{7}\right)$を含んでいる．$\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$は，$\mathbb{Q}$上の 3 次元ベクトル空間である．$\mathbb{Q}(\zeta_7)$は，$\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$上から見ると 2 次元のベクトル空間となっている．

5. おわりに

本稿では，円分多項式，円分体，Gauss sum の性質について述べ，円分体$\mathbb{Q}(\zeta_p)$のベクトル空間としての特徴について論じた．

参考文献

[1] Lawrence C. Washington: Introduction to Cyclotomic Fields, Springer−Verlag (1982).